CompTIA Security+ ITAG: Documentation of Credential and Alignment

Credential Name:	CompTIA Security+ SYO-601
Credential Type:	X Certification ☐ License
Issuer of Credential:	CompTIA
Frequency of Updates:	Every 3 Years
Exam(s) Required:	CompTIA Security+ SYO-601 - https://www.comptia.org/certifications/security
Additional Requirements:	
Current CTAG/TAG: (if applicable)	https://www.ohiohighered.org/sites/ohiohighered.org/files/uploads/transfer/CT2/IT_SCTAI_Align_2016.pdf
Description of content to be evaluated and aligned:	
How long after attainment can credit be awarded?	3 Years
How can receiving institutions verify credential attainment?	Provide proof of credential https://help.comptia.org/hc/en-us/articles/115005190103-Provide-Verification-of-Your-CompTIA-Certifications

Course Name: Security Fundamentals or equivalent
Credit Hours: 3 hours
Course Description: A current overview of both network and Internet based security practices and conventions; including planning, implementing, and managing network security. Through an exploration of security technologies, vulnerability assessment and attack methods this course offers methods to minimize potential security risks by means of organizational policy, education and technology

Postsecondary Learning Outcomes	CompTIA Security+ Exam Obj #s refer to CompTIA Content Numbering System
1. Implement practices to properly harden operating systems and application software on a continuing basis.	2.3 Summarize secure application development, deployment, and automation concepts. 3.1 Given a scenario, implement secure protocols 3.2 Given a scenario, implement host or application security solutions. 3.4 Given a scenario, install and configure wireless security settings.

	3.5 Given a scenario, implement secure mobile solutions. 5.1 Compare and contrast various types of controls.
2. Identify commonly used ports and protocols, in both wired and wireless communications, their vulnerabilities and methods to mitigate those vulnerabilities.	3.1 Given a scenario, implement secure protocols 3.3 Given a scenario, implement secure network designs. 3.4 Given a scenario, install and configure wireless security settings. 3.5 Given a scenario, implement secure mobile solutions.
3. Identify and implement software and hardware tools (IP scanning, packet sniffing, and others) to increase network security.	3.3 Given a scenario, implement secure network designs. 2.7 Explain the importance of physical security controls. 2.6 Explain the security implications of embedded and specialized systems.
4. Conduct risk and vulnerability assessments and implement appropriate plans to mitigate common risks and vulnerabilities.	1.1 Compare and contrast different types of social engineering techniques. 1.2 Given a scenario, analyze potential indicators to determine the type of attack. 1.3 Given a scenario, analyze potential indicators associated with application attacks. 1.4 Given a scenario, analyze potential indicators associated with network attacks. 1.5 Explain different threat actors, vectors, and intelligence sources 1.6 Explain the security concerns associated with various types of vulnerabilities. 1.7 Summarize the techniques used in security assessments. 1.8 Explain the techniques used in penetration testing.
5. Implement procedures to properly log system events, review those logs and audit security settings on a regular basis.	4.5 Explain the key aspects of digital forensics.
6. Explain and implement redundancy planning, disaster recovery and incident response as means to provide business continuity.	2.5 Given a scenario, implement cybersecurity resilience 4.3 Given an incident, utilize appropriate data sources to support an investigation. 4.4 Given an incident, apply mitigation techniques or controls to secure an environment. 5.4 Summarize risk management processes and concepts.
7. Explain the impact of organizational policy, state and federal legislation, and	2.1 Explain the importance of security concepts in an enterprise environment.

environmental controls on security planning.	4.1 Given a scenario, use the appropriate tool to assess organizational security 4.2 Summarize the importance of policies, processes, and procedures for incident response. 5.1 Compare and contrast various types of controls. 5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture. 5.3 Explain the importance of policies to organizational security. 5.5 Explain privacy and sensitive data concepts in relation to security
8. Compare and contrast access control methods including role based, discretionary, mandatory and rule based and implement appropriately to secure network resources.	2.4 Summarize authentication and authorization design concepts. 3.7 Given a scenario, implement identity and account management controls.
9. Summarize and deploy various authentication methods including password based, biometric and certificate-based models.	2.4 Summarize authentication and authorization design concepts. 3.7 Given a scenario, implement identity and account management controls. 3.8 Given a scenario, implement authentication and authorization solutions.
10. Explain general cryptographic concepts including hashing, symmetric and asymmetric encryption, digital certificates and public key infrastructure (PKI)	2.8 Summarize the basics of cryptographic concepts. 3.9 Given a scenario, implement public key infrastructure.
11. Explain secure protocols including Secure Socket Layer (SSL) and IPSec to provide encrypted communication	3.3 Given a scenario, implement secure network designs.
12. Summarize and apply Virtualization and Cloud concepts	2.2 Summarize virtualization and cloud computing concepts 3.6 Given a scenario, apply cybersecurity solutions to the cloud.